AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Canceled)

2. (Previously Presented) An arithmetic apparatus incorporated in a LSI for performing a long integer product-sum arithmetic operation, the arithmetic apparatus comprising:

an arithmetic unit comprising:

an integer based multiplier circuit;

a finite field GF(2^m)-based multiplier circuit logically adjacent to but separated from said integer based multiplier circuit;

an adder circuit shared by the separated integer based multiplier circuit and the finite field GF(2^m)-based circuit and configured to operate on data from either the integer based multiplier circuit or the finite field GF(2^m)-based circuit; and

a selector configured to select one of said integer multiplier circuit and said finite field GF(2^m)-based multiplier circuit, and

a controller controlling said selector to make said selection.

3. (Currently Amended) An apparatus according to claim 2, wherein ~~the arithmetic unit further comprises~~:

[[an]] the adder circuit ~~which~~ has a buffer for storing interim result data, adds the interim result data to result data from one of said integer based multiplier ~~unit arithmetic~~ circuit and said finite field ~~GF(2^m) based unit arithmetic~~ GF(2^m)-based multiplier circuit which is selected by said selector, propagates a carry in an integer based unit arithmetic operation, and propagates no carry in a finite field GF(2^m) based unit arithmetic operation.

4. (Previously Presented) An apparatus according to claim 3, wherein the arithmetic unit further comprises:

a carry holder for storing a carry obtained in a previous operation cycle, and an output-stage adder circuit configured to add the carry in said carry holder to an output from said adder circuit, output an upper bit of an addition result as an updated carry to said carry holder, and output a lower bit of the addition result as operation result data.

5. (Previously Presented) A crypto processing apparatus for selectively encrypting or decrypting based on an integer based operation by said arithmetic apparatus defined in claim 2, and encrypting or decrypting based on a finite field GF(2^m) based unit arithmetic operation by said arithmetic apparatus.

6-19. (Canceled)